APPENDIX C. ESTIMATING THE WAITING TIME UNTIL THE SIMULTANEOUS COLLAPSE OF TWO CONTINGENCIES[1]

(Adapted from Author's Text)

C.1 Introduction. This appendix provides an interface between criticality safety and safety analysis. Recent emphasis calls for probabilistic safety assessments in addition to the traditional qualitative and quantitative, but deterministic, assessments. That emphasis supplies the motive for this appendix, which is narrowly focused on the Double-Contingency Principle (DCP) as applied in criticality safety practice.

C.1.1 DCP Review. The definition of the DCP is stated as, "Process designs shall, in general, incorporate sufficient factors of safety to require at least two unlikely, independent, and concurrent changes in process conditions before a criticality accident is possible." For example, given a fissile material workstation in a glovebox, the "two unlikely" events are inadvertent double-batching and inadvertent flooding with water. In this example, work begins at the workstation at time zero. The purpose of this probabilistic model is to make a probabilistic statement about the waiting time until the workstation is simultaneously flooded and double-batched.

C.1.2 Markov Model. A Markov model is convenient and tractable. In such a model, (1) the time span from recovery from a flooded condition to onset of the next flooded condition is an exponentially distributed random variable, (2) the time span from the onset of a flooded condition to recovery from that flooded condition is an exponentially distributed random variable, and (3) those two random variables are independent. A similar set of statements applies to the double-batching situation.

C.1.3 Probabilistic Description. Given estimates of mean failure and mean recovery times of the two independent contingencies, the model can be used to generate a probabilistic description of the waiting time to the first simultaneous collapse; or, if estimates of mean failure and mean recovery times of the two independent contingencies are unavailable, the model can be used to construct parameter surveys to bound estimates that could satisfy a criterion for mean time to simultaneous collapse.

C.2 General Markov Model. The construction of a Markov model for the general situation follows. For k = 1, 2, let $X_k(t) = 1$ if contingency k is in its desired state; let $X_k(t) = 0$ if contingency k is in its undesired state. Suppose that at time zero both contingencies are in the desired states: $X_1(0) = 1$ and $X_2(0) = 1$. For k = 1, 2, let $1/\lambda_k$ be the mean time between transitions from desirable to undesirable states for the k^{th} contingency. Similarly, let $1/\mu_k$ be the mean time between transition from undesirable to desirable states. If the Markov model is invoked, then the sojourns between transitions are independent, exponentially distributed random variables. The process is assumed to begin in state (1,1) (i.e., $X_1(t) = 1$ and $X_2(t) = 1$). The waiting time until the first visit to state (0,0) (i.e., $X_1(t) = 0$ and $X_2(t) = 0$) is to be determined. That waiting time is also a random variable to be determined as follows.

The (0,0) state is that in which both contingencies are in undesired states, and in practice, is a state from which exit is possible. However, it is convenient for modeling purposes to make (0,0) an absorbing state, one from which exit is not possible. If state (0,0) is an absorbing state and T, a

random variable, is the waiting time until the first visit to (0,0), given that the process begins in state (1,1); then for any $t > 0$, the events $[T \leq t]$ and $[X_1(t) = 0 \text{ and } X_2(t) = 0]$ are equivalent. That equivalence simplifies the following mathematical demonstration.

Figure 1 displays a state transition diagram for the two-state Markov process. For $i = 0,1$ and $j = 0,1$; let $P_{ij}(t) \equiv P[X_1(t) = i \text{ and } X_2(t) = j]$. The incantation that corresponds to the right hand side of the last definition is "probability that X_1 at time t equals i and X_2 at time t equals j." Then from the figure, the system of first order differential equations that the P_{ij} satisfy is

$$\left.\begin{aligned} \frac{dP_{11}}{dt} &= -(\lambda_1 + \lambda_2) P_{11} + \mu_1 P_{01} + \mu_2 P_{10} \\ \frac{dP_{10}}{dt} &= -(\lambda_1 + \mu_2) P_{10} + \lambda_2 P_{11} \\ \frac{dP_{01}}{dt} &= -(\lambda_2 + \mu_1) P_{01} + \lambda_1 P_{11} \\ \frac{dP_{00}}{dt} &= \lambda_1 P_{10} + \lambda_2 P_{01} \end{aligned}\right\} \qquad (1)$$

Since the process begins in state (1,1), the initial conditions for system (1) are: $P_{11}(0) = 1$, $P_{10}(0) = 0$, $P_{01}(0) = 0$, $P_{00}(0) = 0$.

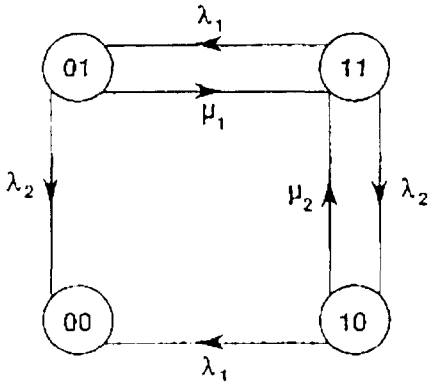

Figure 1. The state transition diagram for the Markov model of the double-contingency stochastic process; "1" is a desirable state, and "0" is an undesirable state.

The technique used for constructing a solution to system (1) is the Laplace transform. Let L represent the Laplace transform operator, and for $i = 0, 1$ and $j = 0, 1$ let $f_{ij} = L\, P_{ij}$. The application of L to system (1) yields

$$\begin{bmatrix} s+\lambda_1+\lambda_2 & -\mu_2 & -\mu_1 & 0 \\ -\lambda_2 & s+\lambda_1+\mu_2 & 0 & 0 \\ -\lambda_1 & 0 & s+\lambda_2+\mu_1 & 0 \\ 0 & -\lambda_1 & -\lambda_2 & s \end{bmatrix} \begin{bmatrix} f_{11} \\ f_{10} \\ f_{01} \\ f_{00} \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} \qquad (2)$$

Solving system (2) for f_{00} yields:

$$f_{00}(s) = N(s)/D(s) \tag{3}$$

where

$$N(s) = (2\lambda_1 \lambda_2)s + (\lambda_1 \lambda_1 \lambda_2 + \lambda_1 \lambda_2 \lambda_2 + \lambda_1 \lambda_2 \mu_1 + \lambda_1 \lambda_2 \mu_2) \tag{4}$$

and

$$D(s) = s[s^3 + (2\lambda_1 + 2\lambda_2 + \mu_1 + \mu_2)s^2 + (\lambda_1 \lambda_1 + \lambda_2 \lambda_2 + 3\lambda_1 \lambda_2 + \lambda_1 \mu_1 + \lambda_1 \mu_2 + \lambda_2 \mu_1 + \lambda_2 \mu_2 + \mu_2 \mu_2)s + (\lambda_1 \lambda_1 \lambda_2 + \lambda_1 \lambda_2 \lambda_2 + \lambda_1 \lambda_2 \mu_1 + \lambda_1 \lambda_2 \mu_2)] \tag{5}$$

Equations (4) and (5) are unnecessarily expanded to highlight the symmetry of the subscripts.

The Laplace transform of $P[T \leq t]$ is f_{00}, and $P[T \leq t]$ is the cumulative distribution function (CDF) that describes T, the waiting time until the simultaneous occurrence of the two contingencies. Hence, a fundamental property of Laplace transforms and the fact that $P[T \leq 0] = 0$ imply that s $f_{00}(s)$ is the Laplace transform of d/dt $P[T \leq t]$. But d/dt $P[T \leq t]$ is the probability density function (PDF) that describes T; let f_T represent that PDF, and let $g_T \equiv Lf_T$. Then from (3):

$$(Lf_T)(s) = g_T(s) = \frac{sN(s)}{D(s)} \equiv \frac{N(s)}{D^*(s)} \tag{6}$$

where the last equation in (6) defines D^*.

To invert g_T requires finding roots of the cubic D^*; the coefficients of D^* appear in (5). In application where the λ_i and the μ_i are assigned numerical values, computer-based root finding routines could be used; and f_T could be found by inverting g_T.

Although inversion of g_T is unproductive in the general case, useful information can be extracted from g_T without inversion. That is;

$$g_T(s) \equiv \int_0^\infty f_T(t)\ e^{-st} dt = \langle e^{-sT} \rangle \tag{7}$$

where $\langle\ \rangle$ represents expectation. Hence g_T is a moment generating function for T. In particular, if exp(-st) is expanded in a Taylor series about 0, it is found that $\langle T \rangle = -g'_T(0)$ where the prime represents differentiation with respect to s. Differentiation and algebraic manipulation applied to (4),(5), and (6) yields:

$$\langle T \rangle = \frac{\lambda_1\lambda_2 + \lambda_1\lambda_2 + \lambda_1\lambda_2 + \lambda_1\mu_1 + \lambda_1\mu_2 + \lambda_2\mu_1 + \lambda_2\mu_2 + \mu_1\mu_2}{\lambda_1\lambda_1\lambda_2 + \lambda_1\lambda_2\lambda_2 + \lambda_1\lambda_2\mu_1 + \lambda_1\lambda_2\mu_2} \tag{8}$$

Equation (8) is presented in the expanded form to highlight the symmetry of the relationship.

A special case of (8) is enlightening. In practical cases, if application of the double contingency principle is to yield significant safety advantage, the mean times of transition from desirable to undesirable states should be much longer than the mean times of transition from undesirable to desirable states. In the context of the model, this translates into the assertion that for every i = 1, 2 and j = 1, 2, $\lambda_i \ll \mu_j$. In this special case (8) becomes

$$\langle T \rangle \equiv \frac{\left(\frac{1}{\lambda_1}\right)\left(\frac{1}{\lambda_2}\right)}{\left(\frac{1}{\mu_1}\right) + \left(\frac{1}{\mu_2}\right)} \tag{9}$$

The advantage to be gained by using two contingencies instead of one contingency is demonstrated in the following quantitative estimate of examining the mean time to the first simultaneous occurrence of two contingencies. Suppose $1/\lambda_1 = 5$ years, $1/\lambda_2 = 10$ years, $1/\mu_1 = 5$ days, and $1/\mu_2 = 2$ days. Then equation (9) applies, and $\langle T \rangle \approx 2600$ years; the advantage is substantial in this case.

Equation 8 is provided for the general case and equation 9 is provided for the special (and usually applicable) case.

C.3 Symmetric Case. The "symmetric case" is for circumstances in which both contingencies are described by identical probabilistic models, i.e., $\lambda_1 = \lambda_2 \equiv \lambda$ and $\mu_1 = \mu_2 \equiv \mu$. The symmetric case can be treated as above by starting with a state transition diagram and writing down the corresponding first-order linear system of differential equations. The system is 3 x 3 matrix instead of 4 x 4 matrix because the states (0,1) and (1,0) are indistinguishable.

The symmetric case is logically equivalent to what reliability theorists call the two-unit-active-redundant case, and it has been completely solved[2,3] and is provided as follows.

As before, let T be the waiting time until the first visit to state (0,0). Then for time $t \geq 0$,

$$P[T > t] = \frac{\sigma_2 e^{-\sigma_1 t} - \sigma_1 e^{-\sigma_2 t}}{(\sigma_2 - \sigma_1)} \tag{10}$$

where

$$\left.\begin{aligned} \sigma_1 &= \frac{1}{2}\left[(3\lambda + \mu + \sqrt{\mu^2 + 6\lambda\mu + \lambda^2}\,\right] \\ \sigma_2 &= \frac{1}{2}\left[(3\lambda + \mu + \sqrt{\mu^2 + 6\lambda\mu + \lambda^2}\,\right] \end{aligned}\right\} \tag{11}$$

and

$$\langle T \rangle = \frac{1}{2}\left[3 + \frac{\left(\frac{1}{\lambda}\right)}{\left(\frac{1}{\mu}\right)}\right]\left(\frac{1}{\lambda}\right) \tag{12}$$

Equation (10) is a complete probabilistic description of T. To obtain a corresponding result for the asymmetric case requires finding the roots of the cubic D' defined in equation (6).

Although there is no simple equivalent of (10) for the asymmetric case, equation (10) may be conservatively used in the asymmetric case by setting $\lambda = \max(\lambda_1, \lambda_2)$ and $\mu = \min(\mu_1, \mu_2)$. Such an application may be useful to gain quick insight and might even suffice without further analysis if the result satisfies the preset criterion.

REFERENCES

1. C. S. Barnett, "A Probabilistic Model for Estimating the Waiting Time Until the Simultaneous Collapse of Two Contingencies," *Proc. International Conference on Nuclear Criticality Safety*, Dorset, England, September 9-13, 1991.

2. B. Epstein and J. Hosford, "Reliability of Some Two-Unit Redundant Systems," *Proc. Sixth National Symp. Reliability and Quality Control* (January, 1960), 469-488.

3. N. J. McCormick, "Reliability and Risk Analysis," P 143, Academic Press, Inc., 1981.